12 FAM 620 UNCLASSIFIED AUTOMATED INFORMATION SYSTEMS

(TL:DS-87; 01-08-2003)
(Office of Origin: DS/IST/ACD)

12 FAM 621 PERSONNEL SECURITY

12 FAM 621.1 General

(TL:DS-69; 06-22-2000)

a. The Department of State has established personnel security procedures to ensure that all personnel accessing Department automated information system (AIS) processing resources have:

(1) The required access levels and need-to-know;

(2) Appropriate supervision; and

(3) Knowledge of their AIS security responsibilities.

b. Procedures and requirements that appear in this section implement the personnel security program for all of the Department's unclassified AISs, regardless of hardware platform, in both the domestic environment and the environment abroad.

12 FAM 621.2 Background Investigations and Personnel Selection

12 FAM 621.2-1 Domestic

(TL:DS-69; 06-22-2000)

a. Only individuals who meet the requirements for sensitive positions outlined in the 3 FAM 2222 may be members of the systems staff or users with special access privileges, such as operator privileges.

b. The data center manager and the information systems security officer

(ISSO), for nonmainframe AISs, must ensure that a limited background investigation (LBI) is performed for all uncleared vendor maintenance personnel by the Office of Investigations and Counterintelligence (DS/ICI/PSS). See 12 FAM 629 for additional information.

12 FAM 621.2-2 Abroad

(TL:DS-69; 06-22-2000)

a. The administrative officer and the IMO or IPO identify all AIS system staff positions at post and determine the sensitivity level of each position.

b. The regional security officer (RSO) or post security officer (PSO) performs the highest level background investigation available at post on all third-country nationals (TCNs), Foreign Service nationals (FSNs), local contractors, and part-time U.S. citizen systems staff and application users with special access privileges, such as those with backup operator privileges.

c. The RSO or PSO performs the highest level background investigation available at post on local vendor contract maintenance personnel.

d. The data center manager and the system manager positions at posts responsible for running the financial management system (FMS) are sensitive positions. The administrative officer must ensure that U.S. citizen personnel fill these positions.

12 FAM 621.3 Personnel Management

12 FAM 621.3-1 Performance Evaluations

(TL:DS-69; 06-22-2000)

Supervisors must include a statement specifying responsibilities for AIS system security in job and work requirements statements for computer operations staff and program managers who have responsibility for a specific application, such as FMS.

12 FAM 621.3-2 Separation of Duties

(TL:DS-69; 06-22-2000)

The ISSO, the data center manager, the system manager, and the user's supervisor must structure user access privileges to reflect the separation of key duties users perform in the function the specific application supports.

Access privileges must be consistent with the separation of duties established for manual processes.

12 FAM 621.3-3 System Access

(TL:DS-69; 06-22-2000)

Personnel officers must include the data center manager and the system manager on the bureau or post check-out list, to ensure notification of all employees (U.S. and non-U.S. citizen) and contractors who are transferred or terminated. The data center manager and the system manager, in conjunction with the ISSO, must revoke user access privileges for these personnel. Personnel officers must notify the data center manager, the system manager, and the ISSO immediately of any employee or contractor with access to the AIS whose employment is being terminated for any reason. See 12 FAM 629 for additional information.

12 FAM 621.3-4 Main Computer Room Access

(TL:DS-69; 06-22-2000)

a. Domestically, the data center manager and the system manager, and abroad, the RSO or PSO, must designate the computer room, which houses the central processing unit (CPU) and associated storage devices, as a limited access area restricted to authorized personnel only.

b. The data center manager and the system manager must limit access to the operating system and application software designated for use on the AIS to system personnel identified on the authorized access list. See 12 FAM 629 for additional information.

c. While in the computer room, uncleared visitors must be under continuous visual observation by a person with authorized unescorted access. See 12 FAM 629 for additional information.

d. The data center manager and the system manager ensures that custodial and building maintenance personnel entering the computer room are under continuous visual observation at all times by a person with authorized unescorted access.

12 FAM 622 ADMINISTRATIVE SECURITY

12 FAM 622.1 Management Control Process

12 FAM 622.1-1 Information Systems Security Officer (ISSO) Designation

(TL:DS-69; 06-22-2000)

a. For each Department AIS, an ISSO must be designated, in writing, to manage the AIS security program. An alternate ISSO must also be designated, in writing, to fulfill these duties in the absence of the ISSO. These requirements apply regardless of the size of the AIS. For nonmainframe AISs, these designations will be made by the executive director for each bureau or office for a domestic AIS, and by the administrative officer for an AIS abroad. For mainframe AISs, these designations will be made by the data center manager in consultation with the Mainframe Security Program manager. For RIMC AISs, these designations will be made by the RIMC director. 12 FAM 622 Exhibit 622.1-1 contains a sample memorandum assigning ISSO responsibilities to an individual.

b. On nonmainframe AISs, the ISSO and alternate ISSO do not have to be system managers. On mainframe AISs, the duties of the ISSO and alternate ISSO must be separate from those of the data center manager.

c. On nonmainframe AISs, the ISSO and the alternate ISSO will have full access to the AIS. On mainframe AISs, the ISSO and alternate ISSO will be given access to only those system functions that are required for them to perform their official duties.

d. In compliance with the Department's Internal Controls Program (see 4 FAM), the ISSO's performance appraisal will be based in part on the effective implementation of information systems security requirements.

e. For mainframe AISs, a copy of the signed memorandums designating the mainframe application ISSO and the alternate mainframe application ISSO must be submitted to IRM/OPS/ITI/SI.

f. IRM/OPS/ITI/SI shall designate, in writing, a Mainframe Security Program manager who will implement and manage the Department’s AIS security program for mainframe AISs. The Mainframe Security Program manager will advise all mainframe application ISSOs on the Department’s mainframe AIS security policies and procedures so that no one mainframe AIS will compromise the security of another. He or she will also facilitate the exchange of information among mainframe ISSOs and will assist them in solving technical or procedural problems. IRM/OPS/ITI/SI shall designate, in writing, an alternate Mainframe Security Program manager to fulfill those responsibilities when the primary Mainframe Security Program manager is absent.

12 FAM 622.1-2 System Access Control

(TL:DS-69;   06-22-2000)

a. The ISSO, on mainframe AISs, and the system manager, on nonmainframe AISs, must control and limit AIS access to the level necessary for users to perform their official duties. See 12 FAM 629 for additional information.

b. Supervisors must complete a system access request form for each staff member who requires AIS access. See 12 FAM 629 for additional information.

c. The ISSO, on mainframe AISs, and the system manager, on nonmainframe AISs, will review annually all AIS users with exceptional access privileges, to ensure that their privileges are still needed in order for the users to perform their official duties.

d. The program manager must review annually the access privileges for each AIS mainframe user with access to an application system/database under their supervision to ensure that the access is still needed in order for the user to perform his or her official duties.

e. When a mainframe AIS application system/database is being accessed by other application systems or by other independent processes, the program manager responsible for the mainframe AIS application system/database must review annually these accesses to ensure that the access is still needed in order for the other application system or independent process to perform its function.

f. The ISSO, on mainframe AISs, must ensure that contractor personnel who have been granted mainframe AIS access retain this access for a specified period of time not to exceed three years. At the end of the specified time period, contractor personnel must make a formal request to the ISSO for their AIS access to be renewed.

12 FAM 622.1-3 Password Controls

(TL:DS-69;   06-22-2000)

a. The data center manager and the system manager must initially assign a unique user ID and password to each new authorized user. If required by the user's work, the data center manager and the system manager may assign more than one user ID and password to the same individual. However, under no circumstances may more than one user be assigned or permitted to use the same user ID and password. Group user IDs and passwords are prohibited. Once the new user has accessed the system for the first time, the user must change the issued password within ten calendar days. See 12 FAM 623.3-1.

b. The data center manager and the system manager may not maintain permanent user IDs and passwords on AISs for visitors, vendor service personnel, training, demonstrations, or other purposes. The approved format for passwords is contained in 12 FAM 623.3-1.

c. The data center manager and the system manager shall distribute initial passwords to users in a secure manner which prevents disclosure to other individuals. The data center manager and the system manager shall make all users aware of the private nature of their passwords. Users must inform the ISSO if they suspect that their passwords have been compromised.

d. Users must acknowledge receipt of their user IDs and their initial passwords by signing a password receipt/security acknowledgement. See 12 FAM 629 Exhibit 629.2-2 for a sample format.

e. The data center manager and the system manager must ensure that all passwords are changed under the following conditions:

(1) At least once every six months;

(2) Immediately following any suspected compromise; or

(3) Whenever someone with system security authority no longer requires that level of access.

To ensure that all passwords are changed every six months, the data center manager and the system manager should either use a tickler file or preferably reconfigure the AIS to require the user to create a new password to maintain access to the AIS after six months.

f. The data center manager and the system manager must immediately delete individual user IDs and passwords under the following conditions:

(1) Whenever notified by a user's supervisor that the user no longer requires AIS access;

(2) Whenever notified by a proper authority, such as the personnel officer, that the user's employment has been terminated with the Department or has been transferred to another office or post; or

(3) Whenever requested by a proper investigative authority or by the supervisor at the request of proper investigative authority pursuant

to a criminal or national security investigation.

g. Program managers must review annually access privileges of each user under their supervision to verify that the privileges originally granted are still appropriate. See 12 FAM 629 for additional information.

h. On AISs, where the password change function has been automated through approved security software, the password change interval must be mandatorily set to six months. Also, if the approved security software supports a "password history feature," this feature must be enabled to retain the last five password generations for each individual user.

12 FAM 622.1-4 Use of Systems

(TL:DS-86; 12-10-2002)

a. The ISSO must ensure that all unclassified AISs are used only for processing unclassified information.

b. The ISSO must inform all AIS users that they must use the most stringent access controls available when processing information concerning an individual that is considered to be compromising, adverse, embarrassing, or derogatory. Users should store such information on the AIS for the minimum amount of time necessary.

c. Domestically, the Office of Medical Services (M/DGHR/MED) must approve all AISs used to process or store medically privileged information (Medical-SBU) protected under the Privacy Act of 1974, 5 U.S.C. 552a (e)(10). These AISs must remain under the direct supervision and control of M/DGHR/MED.

d. Abroad, the regional medical officer or Foreign Service health practitioner in conjunction with the ISSO must ensure that all AISs used to process and store medically privileged information (Medical-SBU) protected under the Privacy Act of 1974, 5 U.S.C. 552a (e)(10), can only be accessed by individuals authorized by the regional medical officer or Foreign Service health practitioner in concurrence with the ISSO. These requirements are in addition to all other applicable controls found in this section that must be implemented for the protection of unclassified AISs.

e. The ISSO must notify all AIS users that personal use of Department AIS equipment is prohibited. Therefore, users do not have a reasonable expectation of privacy in the AIS. The Director, Diplomatic Security Service, may authorize access to special agents of the Department of State and other Federal law enforcement agencies in the conduct of investigations for employee misconduct or the violation of any Federal law. DS/ICI/PSS will coordinate with the affected bureau at an appropriate time in the investigation. See 12 FAM 629 for additional information.

f. The ISSO must instruct all AIS users that, when logged on, workstations are never to be left unattended. All activity occurring when the workstation is functioning is the responsibility of the logged-on user.

g. The data center manager and the system manager will label all AIS peripherals to indicate that the AIS is used for unclassified processing or, at the discretion of the data center manager or system manager in consultation with affected program managers, for Sensitive But Unclassified *(*SBU*)* processing. An SBU label is not required for processing SBU information on an unclassified AIS. Rather, an SBU label serves to increase the awareness of users regarding especially sensitive AISs. Further, either label will alert personnel that classified information may not be processed on the AIS and/or peripherals.

h. Mainframe users must comply with established mainframe operational procedures and guidance issued by IRM/OPS/ITI/SI.

12 FAM 622.1-5 SBU Processing

(TL:DS-69; 06-22-2000)

a. Sensitive But Unclassified (SBU) information may be processed on unclassified AISs, bearing in mind that U.S. citizen and FSN/TCN personnel with system administrator access privileges routinely have the ability and authority to access users' libraries/files in the course of their AIS duties. Supervisory personnel may, at their discretion, direct that subordinates not process especially sensitive information on an unclassified AIS.

b. Unclassified AISs do not need to be certified for processing SBU information.

12 FAM 622.1-6 After-Hours Operations

(TL:DS-69; 06-22-2000)

a. Domestically. For any non-24 hour AIS operating after normal working hours, the ISSO must ensure that appropriate after-hours restrictions are developed and implemented for all AISs under the ISSO's control within a bureau or office.

b. Abroad. For any non-24 hour AIS, users must notify the ISSO and the system manager in advance of any requirement for after-hours use of the AIS. See 12 FAM 629.

(1) For any non-24 hour AIS, U.S. citizen supervisors must authorize in writing any AIS access after normal working hours by Foreign Service nationals (FSNs), third-country nationals (TCNs), or contract employees. Also indicated is the period of time such access is required. All post security requirements for FSN, TCN, or contract employees' after-hours access must also be met.

(2) For any non-24 hour AIS operating after normal working hours, the system manager will connect only those workstations required for use to the central processing unit. See 12 FAM 629.

c. Logs. The data center manager and the system manager must ensure that all system logs in effect during normal operations are also activated during after-hours operations.

12 FAM 622.1-7 Protection of Media and Output

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager must store all operating system and application software under his or her control in a locked area or approved security container. Unclassified media under the control of AIS users (e.g., diskettes) do not have to be secured during working hours but, after hours, must be appropriately stored by the users out of view in a desk or cabinet. The users of medically privileged information must ensure that this information is secured when not in use.

b. Domestically, the ISSO and, abroad, the RSO or PSO must review and approve all locally established procedures for transportation and control of media. Media procedures include:

(1) Domestically: This media must remain under the control of a cleared Department of State or contract employee during transport or be shipped via U.S. registered mail; and

(2) Abroad: Media shipped between posts must be sent at a minimum by controlled shipment. Media may be hand-carried between posts by a U.S. citizen providing the media remains in his or her possession at all times.

c. The data center manager and the system manager must label all removable media either UNCLASSIFIED or SBU. Whereas media containing sensitive but unclassified information does not necessarily have to be marked SBU, the owner(s) (program manager(s)) of the information should be consulted regarding whether or not an SBU marking is warranted instead of an UNCLASSIFIED marking. The “NOFORN” caption and distribution restriction may also be added when the information warrants a higher level of protection.

12 FAM 622.1-8 Monitoring System Users

(TL:DS-69; 06-22-2000)

a. The ISSO conducts reviews of randomly selected user libraries and word-processing documents on a monthly basis to ensure that users are:

(1) Adequately protecting sensitive information;

(2) Archiving sensitive information;

(3) Maintaining sensitive information on the AIS for the minimum amount of time necessary; and

(4) Not processing classified information on the AIS.

b. The ISSO reviews the list of AIS users on a periodic basis to determine whether all users are authorized access to the AIS.

12 FAM 622.1-9 Security Incident Procedures

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager documents, in the operations log, all security-related abnormal system operations that may result in unauthorized disclosure, loss, or modification of system programs or data.

b. The data center manager and the system manager must immediately notify the ISSO, DS/CIS/IST, and, if abroad, the RSO or PSO, and the regional computer security officer (RCSO), if applicable, of any security-related abnormal system operation.

c. Any AIS user discovering or suspecting incidents of fraud, misuse, disclosure of information, destruction or modification of data, or unauthorized access attempts, must immediately report the incident to the ISSO, the data center manager, or the system manager, and, additionally, if abroad to the RSO or PSO. Domestically, the ISSO, the data center manager or system manager must review the matter and ensure that the results of the review are forwarded to the appropriate

Departmental authorities for resolution. Abroad, the ISSO must provide the RSO or PSO with technical assistance and advice in the conduct of an investigation.

d. In the event of a serious incident that indicates disclosure, modification, destruction, or misuse of AIS resources, the data center manager or the system manager must immediately make a full backup copy of the AIS for review. Domestically, the ISSO must report these events to DS/CIS/IST and make the AIS backup available for review. Abroad, the ISSO must report these events to the RSO or PSO, appropriate Department application developers, the RCSO, and/or DS/CIS/IST via telegram and make the AIS backup available for review. If necessary, the ISSO may order all AIS operations to be halted.

12 FAM 622.1-10 Violations

(TL:DS-69; 06-22-2000)

The data center manager, the ISSO on nonmainframe AISs, and, if abroad, the RSO or PSO will look into all known or suspected incidents of noncompliance with 12 FAM 500 and inform management of the results. Management will take necessary and appropriate action to ensure that personnel adhere to these regulations.

12 FAM 622.1-11 Sensitive Media, Output, and Equipment Disposition

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager and ISSO, on mainframe AISs, must ensure that magnetic storage media is not removed from U.S. Government-controlled premises for maintenance purposes, credit, or sale unless all information on the media has been sanitized. See 12 FAM 629 for additional information.

b. The data center manager and the system manager must ensure that procedures are followed for returning damaged disks to the Department for destruction. See 12 FAM 629 for additional information.

c. The data center manager and the system manager must destroy other types of damaged, unclassified magnetic media (e.g., diskettes and tapes) by burning, disintegration, or other methods of destruction approved by the RSO, PSO, or DS/CIS/IST.

d. DS/CIS/IST will furnish detailed instructions concerning the cleaning, repair, and destruction of nonremovable media upon request.

12 FAM 622.1-12 System Maintenance

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager or appointed designee must supervise vendor maintenance personnel accessing AIS equipment at all times.

b. The data center manager and the system manager will prohibit maintenance personnel from running remote diagnostics on any Department or post AIS from an off-site location.

c. The data center manager and the system manager will ensure that a log is maintained of all maintenance or service performed on the AIS. See 12 FAM 629 for additional information.

12 FAM 622.1-13 Security Reviews and Reports

(TL:DS-69; 06-22-2000)

a. DS/CIS/IST will conduct periodic security evaluations of all unclassified AISs, regardless of hardware platform. These evaluations address implementation of and compliance with applicable Federal and Department AIS security policies, procedures, and requirements. See 12 FAM 629 for additional information.

b. IRM/OPS/ITI/SI will conduct ongoing monitoring and technical auditing of security controls on Department unclassified mainframe AISs.

c. The Mainframe Security Program manager must ensure that an annual independent audit is performed on the security controls of all mainframe AISs under his or her authority. A copy of the audit findings should be sent to IRM/OPS/ITI/SI.

d. Abroad, the ISSO, in conjunction with the administrative officer, RSO or PSO and other appropriate post personnel, will conduct an annual review of user and system operation practices to evaluate compliance with these regulations. See 12 FAM 629 for additional information.

12 FAM 622.1-14 Review of Audit Logs

(TL:DS-69; 06-22-2000)

Abroad, the ISSO informs the RSO or PSO, and domestically, DS/CIS/IST, of all security-related anomalies discovered during the review of audit logs. See 12 FAM 629 for additional information.

12 FAM 622.2 Training

(TL:DS-69; 06-22-2000)

a. The DS Training Center (DS/PLD/TC) provides AIS security awareness and training materials, to the ISSO, data center manager, system manager, and other Department personnel who have security responsibilities for Department AISs. DS/CIS/IST provides technical course development and training resources.

b. The ISSO, the data center manager and the system manager, as well as the RSO or PSO abroad, must ensure that all personnel with access to the AIS have received site-specific AIS security training. The training must be related to individual responsibilities regarding AIS use or operation.

c. IRM/OPS/ITI/SI will provide mainframe security utility software training to mainframe ISSOs. When necessary, IRM/OPS/ITI/SI will also provide this training to mainframe end users.

d. Department organizations developing software and systems must ensure that programmers receive adequate AIS security awareness training on Department policies and procedures.

12 FAM 622.3 Backup and Contingency Planning

12 FAM 622.3-1 Backup

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager shall implement and document a full backup procedure for system programs and information to ensure continuity of operations.

b. For **all** nonmainframe AISs **administered by the Department of State**, the system manager must place a password giving access to security administrator privileges in a sealed envelope and provide it to the executive director, domestically, and, abroad, to the RSO, IMO, and administrative officer for availability under emergency situations or exceptional conditions. Domestically, the executive director, and abroad, the RSO, IMO, and administrative officer must ensure that this password is stored in a secure location. The system manager will notify the executive director, domestically, and, abroad, the RSO, IMO, and administrative officer in writing if this password is used under emergency or exceptional conditions, and will issue a new password for the backup ID.

c. On **all** mainframe AISs **administered by the Department of State**, IRM/OPS/ITI/SI must place a firecall (emergency) password giving access to security administrator privileges in a sealed envelope and provide it to the data center manager for availability under emergency situations or exceptional conditions. The data center manager must ensure that the firecall password is stored in a secure location. The data center manager will notify the mainframe ISSO and IRM/OPS/ITI/SI in writing when the firecall password is used. IRM/OPS/ITI/SI will then issue a new firecall password to the data center manager.

d. **AISs administered by U.S. Government agencies other than the Department of State will comply with the backup and contingency planning requirements of the responsible agency.**

e. The data center manager and the system manager must identify a secure location to store backup media for AISs to ensure continuity of operations. Any on-site location should be as far away from the information processing facility as possible. The data center manager and the system manager must ensure that alternate storage locations are protected from environmental conditions such as extreme heat, humidity, and air pollution. See 12 FAM 629 for additional information.

12 FAM 622.3-2 Contingency Plan Preparation

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager are responsible for developing a contingency plan for each Department AIS under their authority.

b. The data center manager and the system manager must update each contingency plan annually or when major modifications to the AIS occur. The data center manager and the system manager should test each contingency plan annually, or when major modifications are made. The data center manager and the system manager will inform personnel at backup processing sites of any major modifications to the AIS.

c. The data center manager and the system manager will ensure that IRM/OPS/ITI/SI receives a copy of the contingency plan and any updates to the contingency plan.

d. Domestically, the data center manager, the system manager and the

ISSO will coordinate the contingency plan with the Department's occupant emergency plan to ensure that any emergency response procedures specified in the contingency plan are consistent with the Department's occupant emergency plan.

e. Abroad:

(1) The data center manager and the system manager, in conjunction with the IMO or IPO, and RSO or PSO will coordinate the contingency plan with the post emergency action plan (see 12 FAH-1) to ensure that any emergency response procedures specified in the contingency plan are consistent with the post emergency action plan;

(2) The administrative officer ensures that contingency plans which involve other posts (such as the use of their AISs to provide backup processing capability) are fully coordinated with their administrative officer, RSO or PSO, ISSO, data center manager, and system manager. See 12 FAM 629 for additional information.

12 FAM 622.4 Security Plan Preparation

12 FAM 622.4-1 General Support Systems

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager, in conjunction with the ISSO, is responsible for developing a security plan for all general support systems under their control. (A general support system is defined as an interconnected set of information resources under the same direct management control which shares common functionality.)

b. The data center manager and the system manager, in conjunction with the ISSO, updates each general support system security plan annually or when major modifications to the general support system occur.

c. The data center manager and the system manager, in conjunction with the ISSO, will ensure that IRM/OPS/ITI/SI receives a copy of the general support system security plan and any updates to the general support system security plan for retention in a central repository of such plans.

12 FAM 622.4-2 Major Application Systems

(TL:DS-69; 06-22-2000)

a. The program manager, in conjunction with the data center manager, the system manager and ISSO, is responsible for developing a security plan for each major application system under their control. (A major application is defined as an application that requires special management oversight and attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.)

b. The program manager, in conjunction with the data center manager, the system manager and ISSO, updates each major application system security plan annually or when major modifications to the major application system occur.

c. The program manager, in conjunction with the data center manager, the system manager and ISSO, will ensure that IRM/OPS/ITI/SI receives a copy of the major application system security plan and any updates to the major application system security plan.

12 FAM 622.5 Log and Record Keeping

(TL:DS-69; 06-22-2000)

a. The ISSO, on nonmainframe AISs, and IRM/OPS/ITI/SI, on mainframe AISs, ensures that the following logs and records are maintained for all facilities:

(1) Authorized access lists for AIS facilities;

(2) Visitors logs for the main computer room;

(3) System access requests;

(4) Password receipts/security acknowledgements;

(5) System maintenance logs;

(6) Audit logs;

(7) System operation logs; and

(8) Extended operation logs (if abroad).

b. The ISSO will maintain all logs for at least six months, with the exception of password receipts/security acknowledgement forms, which shall be kept for the duration of the user’s access to that AIS and for six months after the user’s departure.

12 FAM 623 SYSTEMS IMPLEMENTATION

12 FAM 623.1 Operating System and Application Software

(TL:DS-83; 10-07-2002)

Citizens of countries for which DS/DSS/ITA has assessed a critical technical and/or human intelligence threat level shall not develop, modify, or perform maintenance on software used on Department of State computer systems, unless there has been specific DS authorization for each incidence. The information management officer (IMO) responsible for State Department computer systems, both domestically and abroad, must obtain DS/CIS/IST/ACD authorization before such work is begun.

12 FAM 623.1-1 Operating System Software

(TL:DS-69; 06-22-2000)

a. Domestically, the data center manager and the system manager must ensure that DS/CIS/IST is notified prior to installing operating system software, which has never before been installed on any Department multi-user AIS.

b. Abroad, the data center manager and the system manager must ensure that all AISs use only the Department-approved and distributed version of the vendor operating system. IRM will distribute all operating system software to post via controlled shipment.

c. The data center manager and the system manager abroad may only install new releases, upgrades, or patches to the vendor operating system received from the Department. Software received directly from a vendor or a vendor's authorized distributor will not be installed on any post AIS without prior IRM approval.

d. AIS users must not modify operating system software.

e. The data center manager and the system manager must control access to specialized system software, utilities, and functionality that could be used to gain unauthorized access to application data and program code. The data center manager and the system manager will keep access to these resources to the minimum number of authorized users required to accomplish their duties.

f. On domestic mainframe AISs and mainframe AISs abroad, system staff members must not modify operating system software except when installing or applying Department-approved and distributed software updates or fixes. The data center manager must approve all such updates.

g. On domestic mainframe AISs and mainframe AISs abroad, whenever operating system software is installed for which access control is an optional or add-on component, the ISSO must ensure that the access control component or add-on program is installed simultaneously with the operating system software.

h. On domestic mainframe AISs and mainframe AISs abroad, system staff members must not install software products which introduce supervisor calls (SVCs), appendages, authorized programs, interfaces for logging on, facilities for submitting jobs for execution or methods of accessing or transferring data without first ensuring that the products correctly interface with the system security software (e.g., ACF2) and will not adversely affect the security posture of the AIS. The ISSO must ensure that DS/CIS/IST and IRM/OPS/ITI/SI are notified in writing in the event that these requirements cannot be met with respect to any software program product residing on the AIS.

i. On domestic mainframe AISs and mainframe AISs abroad, the ISSO, in conjunction with IRM/OPS/ITI/SI, must ensure that periodic integrity checks are performed on the mainframe system so that:

(1) All vendor-supplied updates or fixes have been reviewed and do not compromise the integrity of the AIS;

(2) All Department programs and routines have been reviewed and do not compromise the integrity of the AIS; and

(3) All new operating systems have been reviewed and do not compromise the integrity of the AIS.

All findings should be reported to the data center manager, IRM/OPS/ITI/SI and DS/IST/ACD.

12 FAM 623.1-2 Application Software

(TL:DS-69; 06-22-2000)

a. Abroad, the data center manager and the system manager must ensure that only Department-approved and distributed versions of application software, other than microcomputer software, are used on AISs. All Department application software must be distributed to posts via controlled shipment.

b. Abroad, the data center manager and the system manager must ensure that all new releases, upgrades, or patches to Department application software installed on post AISs have been approved and distributed by the Department.

c. Department, contractor, and post personnel, other than authorized application developers, may not modify Department standard application software. See 12 FAM 629 for additional information.

d. Department and post personnel may develop application software, provided the application software is developed and documented in accordance with DS and IRM standards. Abroad, all such internally developed application software provided to other posts must be sent by controlled shipment. Domestically, all internally developed application software provided to other offices must remain under Department control during transport or be shipped by U.S. registered mail.

e. The executive director for each bureau or office sponsoring a mainframe AIS application system or database must designate in writing a program manager for each such application system or database.

f. For each Department-sponsored mainframe AIS application system or database, a protection schema must be developed. A protection schema is an outline detailing the type of access users may have to a database or application system, given the user’s need-to-know, e.g., read, write, modify, delete, create, execute and append. This protection schema must include guidelines for granting or denying particular type of access to the application system/database and should be included as part of an application system’s security plan. The program manager must obtain clearance on the protection schema from IRM/OPS/ITI/SI before implementation of the schema. The program manager is responsible for ensuring that the protection schema is enforced by the ISSO.

g. Upon major or minor modifications to a Department-sponsored mainframe AIS application system or database, the program manager will review the protection schema that is in place for the application system/database and make revisions where necessary. The program manager is responsible for informing the ISSO of any revision to the protection schema.

h. The ISSO must implement access controls to the mainframe AIS application or database according to the guidance and instructions of the program manager. In the absence of explicit instructions governing any particular instance of requested access, the ISSO must obtain the approval of the applicable program manager prior to granting access.

12 FAM 623.2 Security Controls

12 FAM 623.2-1 Access Controls

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager must ensure that all security software provided is installed on the AIS. In addition, on mainframe AISs, the ISSO and the data center manager must obtain clearance from IRM/OPS/ITI/SI before installing or upgrading security software.

b. The data center manager and the system manager must ensure that a valid and appropriate logon procedure is assigned that controls the processing options available to each AIS user. See 12 FAM 629 for additional information.

12 FAM 623.2-2 Workstation Restrictions

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager must logically restrict users to workstations and printers on an individual basis.

b. The data center manager and the system manager must ensure that the system automatically disconnects a logged-on workstation or terminal from the AIS or deactivates the keyboard after a predetermined period of inactivity.

c. The data center manager and the system manager must limit unsuccessful logon attempts from any workstation. If the predetermined number of logon attempts is exceeded, the AIS will lock out the workstation. Only the system staff shall have the capability to reset a workstation after lockout.

12 FAM 623.3 Accountability

12 FAM 623.3-1 Identification and Authentication

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager must initially assign each new user a minimum three-character user ID and a minimum six-to-eight character, alphanumeric, randomly generated password. Once the new user has accessed the system for the first time, the user must then change this issued password within ten calendar days, creating a new password according to these specifications:

(1) Password length: The password must be a minimum of eight characters in length. If the system which the user is accessing does not accommodate eight characters, then the user should use the maximum number of character spaces available.

(2) Password composition: The password must be composed of characters from at least three of the following four groups from the standard keyboard:

(a) Upper case letters (A-Z);

(b) Lower case letters (a-z);

(c) Arabic numerals (0 through 9); and

(d) Nonalphanumeric characters (punctuation symbols);

(3) Thereafter, users should construct their own passwords when required: at least once every six months, and when it is suspected that the password has been compromised. The latter must also be reported to the ISSO.

b. For AISs that cannot be configured to filter user-created passwords, it is acceptable for data center managers and system managers to issue machine-generated passwords to users. Any data center manager or system manager without a means to produce machine-generated passwords to distribute may obtain them from IRM/OPS/ITI/SI.

c. Passwords to network devices (e.g., switches, routers) should be constructed and issued as stated in paragraph a of this section or as in paragraph b of this section when the password construction in paragraph a cannot be accommodated.

d. The data center manager and the system manager ensure that users are unable to log on, simultaneously, to the AIS more than once with the same user ID. The data center manager and the system manager may assign an additional user ID and password for users to accomplish their functional responsibilities.

e. Group and “guest” user IDs and passwords are prohibited.

12 FAM 623.3-2 Establishing Audit Trails/Logs

(TL:DS-69; 06-22-2000)

The data center manager and the system manager must archive the audit trail to a file with the most stringent access restrictions available. The audit trail must be retained for a period of 6 months. See 12 FAM 629 for additional information.

12 FAM 624 INFORMATION SYSTEM FACILITY SECURITY

12 FAM 624.1 Construction Standards

(TL:DS-83; 10-07-2002)

All new AIS facilities and major renovations to existing AIS facilities must comply with design standards approved by Overseas Buildings Operations (OBO) for posts abroad and by DS/CIS/DO for domestic locations.

12 FAM 624.2 Perimeter Walls

(TL:DS-69; 06-22-2000)

a. Exterior computer room windows must be protected with mylar and, if necessary, window coverings. See 12 FAM 629 for additional information.

b. Domestically, DS/CIS/DO, and abroad, the RSO or PSO will determine the need to alarm or secure these windows based on local conditions.

c. The senior information management officer, the data center manager or the system manager, in conjunction with the GSO, must ensure that computer room and media storage room perimeter walls extend from the structural floor to the structural ceiling. These individuals will also ensure that penetrations of the floor or ceiling are sealed to maintain environmental integrity.

d. The senior information management officer, the data center manager or the system manager, in conjunction with the GSO, must ensure that all openings in perimeter walls of the computer room and the media storage room that are interior to the building, except for doors and windows, and, abroad, larger than 90 square inches (585 square centimeters), are securely screened with 12-gauge expanded metal; and domestically, larger than 96 square inches (624 square centimeters), are securely screened with 9-gauge expanded metal. These individuals must also ensure that any openings or penetrations of perimeter walls that are part of the building's exterior walls have the openings securely sealed to maintain the integrity of the computer room or media room environment. Perimeter walls include areas below raised floors or above suspended ceilings and extend from the structural ceiling to the structural floor.

12 FAM 624.3 Environmental Protection and Access Controls

(TL:DS-69; 06-22-2000)

All facilities must comply with environmental protection and access controls standards contained in 12 FAM 629.

12 FAM 625 MICROCOMPUTER SECURITY

12 FAM 625.1 Physical Security: Access Control and Media Protection

(TL:DS-69; 06-22-2000)

a. The system manager must ensure that microcomputers (i.e., PCs) with nonremovable storage media (i.e., fixed disks) and those with nonvolatile memory are located in an office which is locked with DS-approved locks for after-hours access control.

b. Microcomputers with removable media (e.g., cartridge drives) need not be located in locked offices; however, system users must ensure that removable media from these microcomputers, including floppy diskettes, are appropriately secured.

c. The system manager must ensure that personnel do not configure the default parameters of any software used to access a host computer to permanently store their user ID and password on the microcomputer.

d. Personnel who intend to use U.S. Government portable microcomputers at an off-site location not under the control of the Department of State must inform domestically, the system manager and the ISSO and, additionally, abroad, the RSO or PSO of the intended use before processing any information at an off-site location. The system manager and the ISSO, and additionally, abroad the RSO or PSO, must inform the user of the necessary security measures to adequately protect the information.

e. Personnel who intend to bring U.S. Government portable microcomputers into Department facilities must notify the system manager and the ISSO, and additionally, if abroad, the RSO or PSO. These individuals will inform the user of the necessary security measures to adequately protect the equipment and the information.

12 FAM 625.2 Administrative Security

12 FAM 625.2-1 Authorized Use of Microcomputers

(TL:DS-69; 06-22-2000)

a. Domestically, the system manager must ensure that privately owned software is not installed or processed on U.S. Government microcomputers. The system manager must also ensure that the electronic transfer of vendor shareware or bulletin board software is limited to a stand-alone microcomputer until the system manager performs a review of the software to ensure that it contains no malicious code. Abroad, the system manager must ensure that privately owned, shareware, or bulletin board software is not installed or processed on U.S. Government microcomputers.

b. System users must ensure that classified and SBU U.S. Government information is not processed on privately owned microcomputers. Nonsensitive unclassified U.S. Government information may be processed on privately owned microcomputers when approved in advance by a supervisor.

c. The installation of U.S. Government software on privately owned microcomputers is prohibited when in violation of host country law, international copyright law, and/or a licensing agreement. A U.S. citizen direct-hire supervisor must approve in advance each installation of U.S. Government owned software on a privately owned microcomputer, as being for the performance of official business. Media used to install U.S. Government software on a privately owned microcomputer may not subsequently be installed on a U.S. Government computer.

d. Media, e.g., diskettes that have been approved to transfer information from a privately owned microcomputer to a U.S. Government system must be checked for viruses on a standalone U.S. Government microcomputer immediately before the transfer.

e. Media, e.g., diskettes that have been used on a classified computer may not be loaded onto an unclassified computer.

f. The system manager ensures that privately owned computers are not installed or used in any Department of State office building.

g. Abroad, the system manager ensures that the local purchase of off-the-shelf software is randomly procured.

h. The system manager must equip all standalone microcomputers with security enhancement controls as identified by DS and A bureaus, such as software products, host-dependent firmware products, independent processor hardware products, etc.

12 FAM 625.2-2 Removal of Microcomputers, Media, and Software

(TL:DS-69; 06-22-2000)

Personnel are prohibited from removing U.S. Government microcomputers or media from Department premises without the prior written approval of the ISSO and additionally, if abroad, the RSO or PSO.

12 FAM 625.2-3 Telecommuting

(TL:DS-87; 01-08-2003)

Approved telecommuting, i.e., regularly scheduled off-site work at home or at a regional telecommuting center, frequently requires the use of a U.S. Government-owned computer and may also involve connectivity to AIS equipment at the Department. The following requirements, listed elsewhere in various sections of 12 FAM 600, are repeated here for ease of reference. Whereas the implementing instructions for these requirements are continuously being updated to take advantage of and/or address new technological developments, program managers and would-be telecommuters are encouraged to consult with DS/IST/ACD/SSB on computer usage when contemplating new telecommuting agreements.

(1) The computer must be equipped with a C-2 operating system or DS-approved D-2 subsystem;

(2) The computer must be equipped with a virus protection program;

(3) The computer must be equipped with hard drive encryption approved by DS/IST/ACD;

(4) Screen savers must be utilized with a password lockout feature;

(5) Only U.S. Government-owned software may be installed on the computer;

(6) A system administrator must install/configure the above items, to include configuring the system so as not to be bootable from the A: drive;

(7) The telecommuter must be briefed by the sponsoring ISSO regarding the former's security responsibilities related to the use of a U.S. Government-owned computer;

(8) Regular backup of data must be performed;

(9) Telecommuting sites are subject to random AIS compliance audits;

(10) Computers used for the processing of Sensitive But Unclassified information may not be connected to other than another Department system;

(11) If connected to a Department system, the connection must be via a DS-approved encryption product, and the telecommuter's computer may not be connected to any other system, regardless of whether or not sensitive information is processed;

(12) The bureau sponsoring the telecommuting activity is responsible for assessing the level of sensitivity of information to be processed at home and determining what protective measures are warranted there for hardcopy information not on the computer, e.g., a locked container for printed material (classified national security information may not be processed or stored at home under any circumstances (see 12 FAM 500));

(13) Use of a personally owned PC, for non-SBU processing only, requires the sponsoring supervisor's approval; and

(14) In addition to the approval of the administrative officer and chief of mission, telecommuting arrangements require the RSO's approval (3 FAM 2361, paragraph d). RSOs should consult with DS/CIS/IST before approving telecommuting at critical technical or HUMINT threat posts.

12 FAM 626 ADDITIONAL REQUIREMENTS FOR CRITICAL TECHNICAL OR CRITICAL HUMINT THREAT POSTS

12 FAM 626.1 Unclassified Automated Information Systems Processing in Controlled Access Areas at Critical Technical Threat Posts

(TL:DS-69; 06-22-2000)

The following system requirements apply to critical technical threat posts identified by the Office of Intelligence and Threat Analysis (DS/DSS/ITA), regardless of the level of human intelligence threat designation. All AISs processing inside controlled access areas (CAAs) at such posts must adhere to the regulations of this section.

12 FAM 626.1-1 System Equipment

(TL:DS-69; 06-22-2000)

a. Hardware.

(1) The IMO or CPO, and RSO or PSO ensure that all AIS equipment and associated peripherals used in controlled access areas are TEMPEST-certified, listed on the National Security Agency's Endorsed TEMPEST Products List, and IRM/OPS-certified.

(2) The IMO or IPO and ISSO may interchange equipment from IRM/OPS-certified TEMPEST AISs operating in controlled access areas processing unclassified and SBU data with TEMPEST components certified for classified processing.

(3) The IMO or IPO and ISSO may only authorize the use of TEMPEST-certified laser printers inside controlled access areas for the production of hard copy output.

b. Microcomputers. The system manager and ISSO ensure that all unclassified TEMPEST microcomputers use completely removable magnetic media (floppy diskettes and hard disk packs). The magnetic media must be stored in an appropriate security container when left unprotected.

c. Software. The data center manager and the system manager must ensure that software intended for use within controlled access areas is Department-approved and shipped via classified pouch and stored at post in a controlled access area.

d. Media destruction.

(1) The ISSO forwards hard disks, by pouch, to IRM/OPS for

disposition. No IRM/OPS hardware, fixed media, or IRM/OPS-certified removable media may be released except to IRM/OPS for destruction. Disk packs shall be disassembled, degaussed, and the platters sent via classified pouch. If disassembly tools are not available, Winchester and hermetically-sealed packs may be shipped intact. The exteriors of all such packages must be marked "IRM/OPS for Destruction" and bear the appropriate classification.

(2) The ISSO must remove the drum from a laser-printer cartridge and sand all of the photoreceptor material off the drum prior to disposal of the cartridge. Once this is accomplished, the cartridge and the drum may be disposed of as unclassified waste.

12 FAM 626.1-2 Zone of Control and Separation Requirements

(TL:DS-69; 06-22-2000)

See requirements contained in 12 FAH-6, *OSPB Security Standards and Policy Handbook.*

12 FAM 626.1-3 System Access

(TL:DS-69; 06-22-2000)

a. Usage. The RSO or PSO and ISSO ensure that all personnel accessing AIS equipment housed in controlled access areas have at least Secret clearances.

b. Maintenance. The RSO or PSO validates the authorization and Top Secret clearance of personnel performing AIS maintenance.

12 FAM 626.1-4 Connectivity

(TL:DS-69; 06-22-2000)

a. The data center manager and the system manager and IPO or IMO must ensure that there is no connectivity from an unclassified AIS to a classified AIS.

b. The IPO or IMO and ISSO must ensure that system circuits, cable housings, and power installations for classified distributed AISs are installed in accordance with the National COMSEC Information Memorandum (NACSIM 5203), "Guidelines for Facility Design and Red/Black Installation."

c. While cable runs for AISs completely within the controlled access area do not require the use of a protected distribution system, the data center manager and the system manager and IPO must ensure that signal lines are readily available for visual inspection.

d. The IPO, the data center manager, the system manager, and the ISSO must ensure that AISs and peripherals located outside a controlled access area (CAA) are not connected to AISs or peripherals located inside a controlled access area. Exceptions for Department Telecommunication System (DTS) connectivity and connectivity to out-of-country or nonembassy systems may be granted on a case-by-case basis with the approval of the Diplomatic Security Service (DSS).

e. The data center manager and the system manager and IPO ensure that cable runs between nonadjacent CAAs are equipped with IRM/OPS-approved encryption devices.

12 FAM 626.2 Unclassified Automated Information Systems Processing Outside Controlled Access Areas at Critical Technical Threat Posts

(TL:DS-69; 06-22-2000)

The following system requirements apply to critical technical threat posts, regardless of the level of human intelligence threat designation. All mainframe and non-AISs processing outside controlled access areas (CAAs) at such posts must adhere to the rules within this section.

12 FAM 626.2-1 System Equipment

(TL:DS-69; 06-22-2000)

a Software.

(1) The data center manager and the system manager may install only Department-issued software sent to post via controlled shipment.

(2) The RSO or PSO and ISSO must securely store all operating system and application software media designated for use on the CPU and ensure that only U.S. citizens with at least a Secret clearance have access.

(3) Users, the data center manager and the system manager may not use magnetic media that has been out of Department or U.S. Government control on DOS systems unless it has been reviewed

and approved by DS/CIS/IST or the tenant agency's cognizant AIS security office.

b. Media destruction.

(1) The ISSO must ensure that hard disks used on AISs operationally accessed only by cleared U.S. citizens are not returned to the vendor for credit. These disks must be repaired on site by authorized technicians or returned to the Department according to procedures outlined above.

(2) To return damaged hard disks used on AISs operationally accessed by FSNs and cleared U.S. citizens to the vendor for credit, post should follow procedures outlined in 12 FAM 629.2-5.

(3) The ISSO must destroy all printer ribbons in accordance with current DS-approved destruction procedures (i.e., burned, shredded, or disintegrated).

12 FAM 626.2-2 System Access

(TL:DS-69; 06-22-2000)

a. Usage

(1) System staff personnel whose duties require access to system supervisory functions must be at least Secret-cleared U.S. citizens.

(2) The data center manager, the system manager and ISSO must restrict unescorted access to rooms housing distributed AIS CPUs, disk drives and AIS media to Secret-cleared U.S. citizens with a valid need-to-know. Escorted access must be by at least Secret-cleared U.S. citizens who are on the computer room unescorted access list.

(3) The data center manager and the system manager, in consultation with the appropriate supervisor, must structure FSN and TCN user profiles to permit minimum user access.

(4) The data center manager and the system manager may not allow FSN or TCN personnel to program or modify software for use on local AISs.

(5) Supervisors and the RSO or PSO must ensure that after-hours use of the AIS by FSN or TCN personnel is directly supervised by at least a Secret-cleared U.S. citizen.

b. Maintenance. The data center manager and the system manager or a cognizant U.S. citizen designee with at least a Secret clearance must supervise Foreign Service national or third-country national personnel performing system maintenance within the computer room.

12 FAM 626.2-3 Connectivity

(TL:DS-69; 06-22-2000)

a. The data center manager, the system manager and the IPO must ensure there is no connectivity to a classified AIS.

b. The IPO, data center manager, system manager, and ISSO must ensure that system circuits, cable housings, and power installations for classified distributed AISs are installed in accordance with the National COMSEC Information Memorandum (NACSIM 5203), "Guidelines for Facility Design and Red/Black Installation."

c. With the exception of DTS connections, the IPO, ISSO, and RSO or PSO must ensure that cable runs for unclassified AISs do not pass through controlled access areas.

d. The IPO, ISSO, and RSO or PSO must ensure that AISs and peripherals located outside controlled access areas do not connect with AISs or peripherals located inside controlled access areas. Waivers for DTS AIS connectivity and connectivity to out-of-country or nonembassy AISs may be granted on a case-by-case basis with the approval of the Diplomatic Security Service.

12 FAM 626.3 Unclassified Automated Information Systems Processing at Critical Human Intelligence Threat Posts

(TL:DS-69; 06-22-2000)

The following system requirements apply to critical human intelligence threat posts not concurrently bearing critical technical threat designation. All mainframe and nonmainframe AISs processing at such posts, both inside and outside controlled access areas, must adhere to the regulations which follow.

12 FAM 626.3-1 System Equipment

(TL:DS-69; 06-22-2000)

a. The data center manager, the system manager and the ISSO may use only hardware and software received by classified pouch shipments inside controlled access areas.

b. The data center manager, the system manager and the ISSO may use only software received by controlled air pouch shipments on AISs outside controlled access areas.

12 FAM 626.3-2 System Access

(TL:DS-69; 06-22-2000)

a. Use

(1) System staff personnel whose duties require access to system supervisory functions must be at least Secret-cleared U.S. citizens.

(2) The data center manager and the system manager may not allow FSN or TCN personnel to program or modify software for use on local AISs.

(3) The data center manager and the system manager, in consultation with the appropriate supervisor, must structure FSN and TCN user profiles to permit minimum user access.

(4) Supervisors and the RSO or PSO must ensure that after-hours use of the AIS by FSN or TCN personnel is directly supervised by a U.S. citizen with at least a Secret clearance.

b. Maintenance

The data center manager, the system manager or a cognizant U.S. citizen designee with at least a Secret clearance must supervise Foreign Service national or third-country national personnel performing system maintenance within the computer room.

12 FAM 627 UNCLASSIFIED DOMESTIC TELEPHONE POLICY

12 FAM 627.1 Purpose and Scope

(TL:DS-69; 06-22-2000)

a. The purpose of this policy is to reduce the known vulnerabilities of the

Department's computerized telephone system (CTS) that could be exploited by hackers and intruders and result in fraud, disruptions, degradation of service and technical eavesdropping.

b. All responsible personnel must implement the controls in this section as they apply to specific installed CTS.

c. The AIS security requirements of this subchapter apply unless later issuance of this subchapter (indicated by transmittal letter number and date) modify or change these requirements.

12 FAM 627.2 System Maintenance

(TL:DS-69; 06-22-2000)

a. Unless in an emergency, ISSO must ensure that all calls between the remote diagnostic facility (RDF) and the Department’s CTS are encrypted with NSA-approved encryption devices.

b. The ISSO must ensure that if a remote diagnostic procedure is required over an unsecured link, the following restrictions are adhered to:

(1) The remote diagnostic facility must not be able to access the CTS system except through a port dedicated to infrequent remote diagnostic activity;

(2) All telephone lines installed to allow access to PBX diagnostic ports must be protected by U.S. Government approved encryption devices, whether or not the lines are in use or the ports are active. Where the operational failure of an encryption unit prevents the use of a line or circuit, the encryption unit(s) may be temporarily removed for the period of time required for expeditious repair or replacement. When such action is necessary, authorization must be obtained from the ISSO or the Chief of IRM/OPS;

(3) A connection may be established only by a call to the RDF by authorized personnel from a designated station inside the technical operations center (TOC) for the Department’s CTS;

(4) In Department-controlled facilities, system software or hardware may be changed only by designated. Only these individuals are permitted physical access to the programming stations.

c. The ISSO must ensure that a secure method is used to identify and authenticate off-site maintenance personnel. If passwords are used, the ISSO will provide off-site maintenance personnel with a one-time password to allow remote diagnostic on the DOS CTS system. The system manager will remove the password upon completion of the diagnostic call. All passwords transmitted between DOS facilities and a remote maintenance facility, and vice versa, must be encrypted.

d. At Department-controlled facilities, the Chief of the data/Voice Services Branch (IRM/OPS/ITI) must provide the ISSO with a list of remote maintenance personnel that have been authorized to perform diagnostics on the CTS system.

12 FAM 627.3 Review of Audit Logs

(TL:DS-69; 06-22-2000)

a. The ISSO should review monthly the call detail reports provided by the CTS for the following indications of fraud or attempted fraud:

(1) Numerous inbound calls of a very short duration;

(2) Outbound calls of long duration;

(3) A noticeable increase of calls during off-peak hours;

(4) A high volume of calls to locations not typically called by the Department;

(5) Numerous calls to any specific location;

(6) Much higher than normal long distance toll charges; and

(7) Calls to unauthorized areas (900 numbers).

b. Any indication of fraud or attempted fraud should be reported to the Office of the Inspector General.

12 FAM 627.4 CTS Switch System Continuity

(TL:DS-69; 06-22-2000)

The data center manager, the system manager and the ISSO must ensure that a procedure is in place to ensure continuity of operations for the domestic CTS system.

12 FAM 627.5 System Configuration

(TL:DS-69; 06-22-2000)

The ISSO must ensure that any feature allowing remote or trunk access to the Department CTS system is controlled. The Department services should be accessible only from subscriber stations or equipment.

12 FAM 627.6 Removal of Media

(TL:DS-69; 06-22-2000)

The ISSO must approve the removal of all contractor proprietary magnetic media from Department facilities.

12 FAM 627.7 System Software

(TL:DS-69; 06-22-2000)

a. The ISSO must ensure a complete copy of all system documentation is kept inside the CTS room. This documentation should include instructions, manuals, service practices, system configuration records, and maintenance records.

b. The ISSO must ensure a log entry is completed when the operating system is reloaded indicating who performed the action and the date and time it was accomplished.

12 FAM 627.8 Additional Security Enhancements

(TL:DS-69; 06-22-2000)

The ISSO should ensure the following enhancements are employed to help maximize the overall security of the CTS:

(1) Positive barriers, such as line or trunk verification and executive override, must be placed into the system to prevent access to features that would allow monitoring of station off-hook audio from outside the CTS;

(2) Central dictation features should be disabled;

(3) Central loudspeaker paging features must only be activated when absolutely necessary;

(4) All operator and programming consoles should be located within the TOC for the Department's CTS;

(5) The number of central answering positions should be minimized;

(6) The CTS and all critical station equipment should be powered by uninterruptable power supplies;

(7) All switching, maintenance or operational conditions set up from a subscriber station should be capable of being selectively canceled at an operator console inside the CTS room.

12 FAM 628 UNCLASSIFIED STAND-ALONE FACSIMILE (FAX) EQUIPMENT

12 FAM 628.1 General

(TL:DS-69; 06-22-2000)

Offices sending and receiving FAX transmissions must adhere to the following security policy to protect U.S. Government information from unauthorized disclosure.

12 FAM 628.2 Management Control Process

12 FAM 628.2-1 Personnel Responsibilities

(TL:DS-69; 06-22-2000)

a. The ISSO for unclassified AISs must ensure that the use of unclassified FAX equipment meets the security requirements of this subchapter.

b. The ISSO must ensure that the following security requirements associated with unclassified FAX transmissions are prominently posted near all functioning unclassified FAX equipment:

(1) Users must be aware that FAX equipment uses commercial telephone lines to process and transmit unclassified data and that these lines are vulnerable to covert monitoring;

(2) Users are responsible for the protection of sensitive and Privacy Act information (see 12 FAM 000 for the definition of Sensitive But Unclassified information);

(3) Any FAX user or FAX recipient discovering or suspecting unauthorized disclosure of information, unauthorized transmission of data, or unauthorized FAX use must immediately report such incidents to the ISSO. The ISSO will assist the RSO or PSO (if

abroad) with appropriate investigatory actions.

12 FAM 628.2-2 Approved Transmission Level

(TL:DS-69; 06-22-2000)

a. The ISSO must ensure all unclassified FAX equipment is clearly labeled, "ONLY UNCLASSIFIED INFORMATION MAY BE PROCESSED ON THIS SYSTEM."

b. In accordance with 12 FAM 556.3, the RSO or PSO must treat the transmission of classified material over unclassified FAX equipment as a security violation.

12 FAM 628.3 Location

(TL:DS-69; 06-22-2000)

Abroad, standalone FAX machines are to be located in rooms where classified information is neither processed nor discussed, and they must be isolated in accordance with TSG standards.

12 FAM 628.4 Additional Requirements for Facsimile Machines Located Inside a CAA

(TL:DS-69; 06-22-2000)

a. The general services officer (GSO) must securely procure FAX equipment for use in the CAA from U.S. vendors in the United States.

b. The ISSO, in coordination with the information management officer (IMO), must ensure the separations requirements addressed in 12 FAH-6*, OSPB Security Standards and Policy Handbook*, are met.

c. At critical threat posts, ISSO and RSO or PSO must ensure that only Top Secret-cleared U.S. citizen personnel install and repair FAX equipment within a CAA.

d. At low, medium, and high technical threat posts, the ISSO and RSO or PSO must ensure that if foreign or third-country national personnel perform FAX equipment maintenance within a CAA they are supervised by appropriately cleared U.S. citizen personnel.

12 FAM 629 GENERAL PROCEDURES

12 FAM 629.1 Personnel Security

12 FAM 629.1-1 Domestic Background Investigations and Personnel Selection

(TL:DS-69; 06-22-2000)

The LBI must consist of a review of a completed security questionnaire, a name check against applicable government, police, credit, and fingerprint records, and include a personal interview if warranted. Under emergency or exceptional conditions, unscreened vendor maintenance personnel may perform maintenance on an AIS under continuous escort by a technically knowledgeable, cleared systems employee.

12 FAM 629.1-2 System Access

(TL:DS-69; 06-22-2000)

The data center manager and the system manager must allow users only limited AIS access until advised in writing by the RSO or PSO that an appropriate background investigation has been completed.

12 FAM 629.1-3 Main Computer Room Access

(TL:DS-69; 06-22-2000)

a. The ISSO, in coordination with the data center manager and the system manager, must develop and maintain a current list of personnel who are authorized unescorted access to the computer room. Domestically, such personnel normally include the data center manager, system manager, operators, and the ISSO. Abroad, such personnel normally include the data center manager, system manager, IRM staff, the ISSO, and security personnel. Programmers and application users do not usually need access to the computer room.

b. The data center manager and the system manager must limit access to the operating system and application software designated for use on the AIS to system personnel identified on the authorized access list.

c. The data center manager and the system manager must maintain a visitors log for all personnel entering the computer room who do not have unescorted access privileges. Only personnel listed on the authorized access list may escort visitors. Individuals not on the authorized access list must sign the visitors log prior to being allowed access to the computer room. See 12 FAM 629 Exhibit 629.1-3 for a sample visitors log.

12 FAM 629.2 Administrative Security

12 FAM 629.2-1 System Access Control

(TL:DS-69; 06-22-2000)

a. On nonmainframe AISs, the system manager grants access privileges in three user categories: system security administrators, system staff, and general users. The access privileges for each category are as follows:

(1) System security administrators (SSAs) have full access to all system functions and all data on the AIS. They are the only users able to modify files containing individual system authentication data. The ISSO must assign SSA privileges to the minimum number of personnel required for effective management of the AIS;

(2) System staff members have access to system devices, programs, and resources; however, this level of access does not permit modification of security parameters or changes to system files containing user authentication data. The ISSO must limit operator privileges, granting them only to members of the system staff who require these privileges to perform their system administration responsibilities; and

(3) General users have access to applications and data files based on supervisor-defined user profiles. This level of system access does not permit operator and system security administrator functions.

b. On mainframe AISs, the ISSO grants access privileges in five user categories: system security administrators, system staff, operations staff, programming staff and general users. The access privileges for each category are as follows:

(1) System security administrators (SSAs), including the ISSO, have full access to all system security functions and all security related data on the AIS. They are the only users able to modify files containing individual system authentication data. SSA privileges must be assigned to the minimum number of personnel required for effective security management of the AIS;

(2) System staff members, including the data center manager, have access to all operating system related devices, programs, and resources. They are the only users authorized to update any component of the operating system. However, they are not permitted access to modify security related data files or files containing user authentication data. System staff privileges must be granted only to members of the system staff who require them to perform their system administration duties;

(3) Computer operations staff (e.g., operators, schedulers and change control technicians) have limited access to operating system related devices, programs, and resources. They control production workflow, allocate machine resources to tasks, monitor system and network performance and service peripheral devices. They are not permitted system security administrator privileges. Operator privileges must be granted only to members of the operations staff who require them to perform their duties;

(4) Programming staff have access to their application-specific programs, libraries, test data files, etc. This level does not permit computer operations, system staff or system security administrator privileges. Programming privileges must be granted only to members of the programming staff who require them to perform their duties; and

(5) General users have access to applications and data files based on program manager defined user profiles. This level of system access does not permit programming, computer operations, system staff or system security administrator privileges.

c. The form must include the user's name, the applications involved, and the type of access required within each application. Whenever a user's functional responsibilities change and the user still requires system access, the user's current supervisor must complete a new system access request form for access privileges commensurate with the user's new responsibilities.

d. The data center manager and the system manager must sign the access request form when the information provided is adequate, indicating approval for AIS access. The data center manager and the system manager retains all approved AIS access request forms for at least six months after the date of removal from the AIS.

12 FAM 629.2-2 Password Controls

(TL:DS-69; 06-22-2000)

a. A sample password receipt/security acknowledgement format is contained in 12 FAM 629 Exhibit 629.2-2. If the system in use cannot be configured to filter user-created passwords, the data center manager and the system manager should not include acknowledgements 1, 2 and 4 of the sample format in the password receipt/security acknowledgement to be signed by AIS users. A user may acknowledge more than one user ID and password on a single form. The data center manager and the system manager must retain copies of all password receipts/security acknowledgements for audit purposes for at least 6 months after the user’s departure.

b. The data center manager and the system manager will provide program managers with any information necessary to aid in the review and will retain written documentation of directed changes.

c. The data center manager and the system manager must delete from the AIS all user IDs and passwords supplied by the vendor during system manufacture and installation, once installation is complete. The data center manager and the system manager must remove default user IDs and passwords, such as "CSG," "System," "Field," and "Test.”

12 FAM 629.2-3 After-Hours Operations

(TL:DS-69; 06-22-2000)

For non-24 hour AISs, the system manager will document all after-hours use of the AIS in a log, which must be retained for a minimum of six months. The system manager must logically disconnect unneeded workstations from the AIS. For those AISs incapable of implementing logical disconnects, the RSO or PSO will determine the need for physical disconnects based on local conditions.

12 FAM 629.2-4 Sensitive Media, Output, and Equipment Disposition

(TL:DS-69; 06-22-2000)

a. The media may be overwritten using the overwrite procedures outlined in the vendor's operations manual or degaussed with a Department-approved magnet. Unclassified media, including sensitive but unclassified media, may also be sanitized by overwriting the entire media three times: once with the binary digit 1; once with the binary digit 0; and once with any single numeric, alphabetic, or special character. Upon completion of the triple overwrite, the media should be randomly checked to ensure that the last character entered is the only readable data on the disk. This can be accomplished by using a low level review utility, e.g., Norton Utilities' hex viewer. These procedures can be accomplished using the operating system. Also, a number of commercial software utilities, e.g., Norton Diskwipe, Governmentwipe, etc., feature this overwrite function.

b. In order to follow contractual procedures for returning damaged fixed disks to the vendor for credit, the data center manager and the system manager should contact IRM/OPS/ITI for the appropriate vendor specific procedures.

c. For returning damaged disks to the Department, the data center manager and the system manager must send to Main State for destruction any damaged, unclassified or SBU magnetic media (fixed disks, disk cartridges, or disk packs) which cannot be returned to the vendor for credit. These disk packs must be disassembled and sent from abroad via controlled pouch or from domestic offices via registered mail or hand-carried to A/OPR/GSM/SSD, Room B-523, Main State. If disassembly tools are not available, Winchester and hermetically-sealed packs may be shipped intact. Packages must be marked "For Destruction."

12 FAM 629.2-5 System Maintenance

(TL:DS-69; 06-22-2000)

The system maintenance log includes the date of service, service performed, software or hardware (including identification numbers) involved, personnel performing the service, equipment removed or replaced, and system condition or status following the service. Records must be retained for a period of 6 months after the date of entry.

12 FAM 629.2-6 Security Reviews and Reports

(TL:DS-69; 06-22-2000)

a. The evaluations consider the threat environment and address post implementation of applicable Federal and AIS security policies, procedures, and requirements.

b. The review includes personnel, administrative, system, and physical security practices. DS/CIS/IST will send posts detailed instructions regarding contents of the report.

12 FAM 629.2-7 Establishing and Review of Audit Trails/Logs

(TL:DS-69;   06-22-2000)

a. The data center manager and the system manager must activate the audit trail capabilities available on the operating system and security software installed on Department or post AISs to record security-related incidents listed in paragraph b of this section. The data center manager and the system manager must also implement any audit trails required by Department organizations for applications running on Department or post AISs.

b. The ISSO must review monthly the audit reports for potential security-related incidents such as:

(1) Multiple logon failures;

(2) Logons after-hours or at unusual times;

(3) Failed attempts to execute programs or access files;

(4) Addition, deletion, or modification of user or program access privileges; or

(5) Changes in file access restrictions.

The ISSO may select additional activities for review based on office or post location and type of information processed.

c. The ISSO must retain all audit logs for a period of six months.

12 FAM 629.2-8 Training

(TL:DS-69;   06-22-2000)

The training must be provided either prior to granting new users access to the system or as soon as possible after access has been granted.

12 FAM 629.2-9 Backup

(TL:DS-69;   06-22-2000)

The storage location should be off-site in a U.S. Government-approved and controlled facility to minimize the potential for complete loss of programs and data should a major catastrophe occur. The system manager may use a secure on-site alternate storage location if a suitable off-site location is unavailable.

12 FAM 629.2-10 Contingency Plan Preparation

(TL:DS-69; 06-22-2000)

Abroad, conditions of mutual backup agreements involving more than one post or agency shall be specified in writing and included in or attached to the contingency plan.

12 FAM 629.2-11 Log and Record Keeping

(TL:DS-69; 06-22-2000)

The data center manager and the system manager must ensure that a system operations log is maintained for all AISs. The log must contain a record of all normal daily operations, system power-up and power-down, media mounted and dismounted, backup and recovery operations, and general environmental conditions. Installation, removal, or modification of system or application software must be noted in the log. Any unusual events or operating conditions must also be noted in the log. The data center manager and the system manager must ensure that logs are maintained for a minimum of six months after the date of the last entry.

12 FAM 629.3 Systems Implementation

12 FAM 629.3-1 Operating System and Application Software

(TL:DS-83; 10-07-2002)

a. The information management officer (IMO), who is responsible for the systems for which development software is being planned, is also responsible for ascertaining the citizenship of the person(s) working on this software project. If any person intending to be hired is a citizen of a country for which DS/DSS/ITA has assessed a critical technical and/or human intelligence threat level, that person shall not be hired for the purpose of developing, modifying, or performing maintenance on software specifically developed for use on Department of State computer systems, unless authorization has been received from the Analysis and Certification Division of the Office of Information Security Technology (DS/CIS/IST/ACD). The IMO must contact DS/CIS/IST/ACD to obtain approval before the work is begun.

b. The IMO should submit the following information to DS/CIS/IST/ACD:

   (1) Name(s) of the individual(s) being considered for performance of

the work;

(2) Name of company/vendor;

(3) Country of citizenship of each applicable individual;

(4) Name and brief description of software;

(5) Purpose of the software, if new; purpose of the maintenance or modification of existing software;

(6) Identification of the destination system (e.g., OpenNet, Classnet, a standalone PC); and whether inside or outside of a controlled access area;

(7) Program language to be used; and

(8) Sensitivity of the data on the destination system.

c. DS/CIS/IST/ACD, in coordination with other DS elements, will conduct an analysis of this information, and prepare a recommendation to allow or not allow the proposed work to commence. All recommendations will be forwarded to the Deputy Assistant Secretary for Countermeasures and Information Security (DS/CIS) for final determination.

12 FAM 629.3-*2* Application Software

(TL:DS-83; 10-07-2002)

The data center manager and the system manager must implement all application controls to ensure that users are assigned access rights and privileges consistent with their functional responsibilities and authorities. Access rights and privileges must be based on need-to-know, separation of duties, and supervisory requirements.

12 FAM 629.3-*3* Access Controls

(TL:DS-83; 10-07-2002)

The data center manager and the system manager must implement file, program, and data access controls to ensure that access to files, programs, and data is limited to users or groups of users with the same need-to-know as determined in conjunction with the user's supervisor. Need-to-know may be based on functional responsibilities, operational requirements, supervisory responsibilities, or on a combination of these factors.

12 FAM 629.4 Information Systems Facility Security

12 FAM 629.4-1 Perimeter Walls

(TL:DS-69; 06-22-2000)

a. Where possible, the senior information management officer, the data center manager or system manager, in conjunction with the GSO, must ensure that computer rooms do not have exterior windows.

b. The senior information management officer, the data center manager or system manager, in conjunction with the GSO, may permit an interior glass wall or window in the computer room to allow system staff personnel to monitor equipment without entering the computer room.

12 FAM 629.4-2 Facility Location

(TL:DS-83; 10-07-2002)

a. The data center manager and the system manager, in conjunction with the GSO and the RSO or PSO, if abroad, and in conjunction with DS/DO, if domestic, must, to the extent possible, locate AIS processing facilities in interior portions of buildings, away from areas subject to frequent use.

b. The data center manager and the system manager, in conjunction with the GSO, and the senior information management officer, if abroad, must locate AIS processing facilities above ground and not beneath areas containing water pipes or subject to water penetration from upper floors, when possible.

c. The data center manager and the system manager, the GSO, and the senior information management officer, if abroad, must locate AIS processing facilities as far away as possible from potential sources of fire such as kitchens, main electrical power distribution panels, and storage areas for combustible materials.

12 FAM 629.4-3 Electrical Power Controls

(TL:DS-83; 10-07-2002)

a. Domestically, the GSO, and abroad, the senior information management officer, the data center manager or system manager, in conjunction with the GSO, must label power distribution panels that supply computer room equipment to indicate the equipment served by the panel. These power panels must be located in an area with adequate protection to prevent accidental or malicious interruption of power to the computer room.

b. Domestically, the GSO, in coordination with DS/DO, and abroad, the senior information management officer, the data center manager or system manager, in conjunction with the GSO, must place an emergency power-off control in a readily accessible location outside the main door to the computer room. Domestically, the GSO should determine the need for a clear plastic cover to protect the emergency power-off control from accidental triggering. Abroad, the emergency power-off control must have a clear plastic cover to protect it from accidental triggering.

c. Domestically, the GSO, in coordination with DS/DO, and abroad, the senior information management officer, the data center manager or system manager, in conjunction with the GSO, must ensure that emergency power-off controls for the AIS processing equipment disconnect power to the main computer room ventilation system as well as the AIS equipment.

12 FAM 629.4-4 Fire Protection and Air Conditioning

(TL:DS-83; 10-07-2002)

a. Domestically, the GSO, and abroad, the senior information management officer, the data center manager or system manager, in conjunction with the GSO, ensure that guidelines and requirements issued by the General Services Administration for domestic sites and by OBO/PE/DE/ADB/FPE for posts abroad are followed in providing fire protection for information processing facilities and media storage areas.

b. Domestically, the data center manager or system manager, in coordination with DS/DO, and abroad, the senior information management officer, the data center manager or system manager, in conjunction with the GSO, must ensure that fire detection systems and alarms in information processing facilities are fully functional at all times. These individuals ensure that fire alarms for the information processing facility annunciate at a location staffed 24 hours a day.

c. Domestically, the GSO, and abroad, the senior information management officer, the data center manager or system manager, in conjunction with the GSO, ensure that air conditioning and humidity controls and gauges are installed in the computer room, as appropriate, to ensure that the environment in the computer room is maintained within the specifications established by the AIS equipment manufacturers.

12 FAM 629.4-5 Locks

(TL:DS-69; 06-22-2000)

a. Domestically.

(1) The ISSO ensures that, at a minimum, each standard access door to the information processing facility is equipped with a DS/CIS/DO-approved push button lock with key override or an electronic card reader or other automated access control system. The ISSO must ensure that the primary door to the computer room is equipped at a minimum with a DS/CIS/DO-approved push-button lock with key override or an electronic card reader or other automated access control system which must be enabled at all times. The ISSO must ensure that all other doors to the computer room are secured from the inside with DS/CIS/DO-approved deadbolt locks or emergency exit panic fixtures.

(2) The ISSO ensures that a DS/CIS/DO-approved push button lock with key override is installed on the doors of all offices which contain workstations with operator console privileges. This lock must be enabled when the computer staff office is left unattended. Override keys are controlled by DS/CIS/DO and may not be issued to office occupants.

(3) The data center manager and the system manager ensures that the combinations for all push-button locks are changed at least every six months, whenever someone with the combination either changes positions or terminates employment with the Department, or the combination has possibly been compromised.

(4) If a separate room is used to store media used in daily operations or for backup, the ISSO must ensure that the primary entrance is equipped with a DS/CIS/DO-approved push-button lock with key override. The ISSO must ensure that all other doors are secured from the inside with DS/CIS/DO-approved deadbolt locks or emergency exit panic fixtures.

b. Abroad.

(1) The SEO installs a DS-approved lock on each door to the information processing facility. The SEO must ensure that the primary door to the computer room is equipped at a minimum with a DS-approved push button lock (e.g., Simplex). This lock must be enabled when the computer room is left unattended. The SEO must ensure that all other doors to the computer room are secured from the inside with DS-approved deadbolt locks (e.g., SM-181). In

addition, either all doors to the computer room or all doors to the information processing facility must also be equipped with DS-approved spin-dial combination locks or DS-approved deadbolt locks for after-hours access control.

(2) The SEO ensures that a DS-approved push-button lock (e.g., Simplex) is installed on the doors of all offices which contain workstations with operator console privileges. This lock must be enabled when the computer staff office is left unattended.

c. Combinations. The RSO or PSO and SEO ensure that the combinations for all locks are changed at least every six months, or whenever someone with the combination changes position, leaves post, or otherwise no longer requires access.

d. Locks. If a separate room is used to store media used in daily operations or for backup, the RSO or PSO must ensure that the primary entrance is equipped with a DS-approved push button lock. The SEO must ensure that all other doors are secured from the inside with DS-approved deadbolt locks.

E. MEDIA STORAGE ROOM. Domestically, the ISSO, and *abroad*, the RSO or PSO must ensure that the room used to store backup media is locked at all times.

12 FAM 629.5 TEMPEST Requirements

(TL:DS-69; 06-22-2000)

See the 12 FAH-6*, OSPB Security Standards and Policy Handbook*, for these requirements.

12 FAM 629.6 Media Destruction

(TL:DS-69; 06-22-2000)

The ISSO forwards all hard disks for disposition by controlled pouch to A/OPR/GSM/SSD, Room B-523. If disassembly tools are not available, Winchester and hermetically-sealed packs may be shipped intact. The exteriors of all such packages must be marked "For Destruction."

12 FAM 622 EXHIBIT 622.1-1 SAMPLE MEMORANDUM OF ASSIGNMENT OF ISSO RESPONSIBILITIES TO AN INDIVIDUAL

(TL:DS-69;   06-22-2000)

Date ____________

UNCLASSIFIED
MEMORANDUM

TO: All Users of Post/Bureau Automated Information Systems

FROM: Post Administrative Officer/Bureau Executive Director

SUBJECT: Designation of the Information Systems Security Officer and the Alternate Information Systems Security Officer

According to 12 FAM 622.1-1, domestically or abroad as applicable, an Information Systems Security Officer (ISSO) must be designated in writing to manage the information system security program (post or bureau). An alternate ISSO must also be appointed to fulfill these responsibilities during periods when the ISSO is absent.

All users of automated information systems (post or bureau) are advised that (name of designee) has been appointed as the ISSO to manage the information system security program. (Name of alternate designee) has been appointed to fulfill these responsibilities during periods when the ISSO is absent.

Please contact the ISSO or alternate ISSO if you have any questions or concerns regarding your automated information system.

12 FAM 629 EXHIBIT 629.1-3
SAMPLE FORMAT FOR A VISITORS LOG

(TL:DS-69;   06-22-2000)

TIME	TIME	NAME	DATE	PURPOSE	ESCORT'S
IN	OUT			OF VISIT	INITIALS

1) ....
....

2) ....
....

3) ....
....

4) ....
....

5) ....
....

6) ....
....

7) ....
....

8) ....
....

9) ....
....

10) ....
....

11) ....
....

12) ....
....

13) ....
....

14) ....
....

15) . . . .
. . . .

16) . . . .
. . . .

17) . . . .
. . . .

18) . . . .
. . . .

19) . . . .
. . . .

20) . . . .
. . . .

12 FAM 629 EXHIBIT 629.2-2 SAMPLE FORMAT OF A PASSWORD RECEIPT/SECURITY ACKNOWLEDGEMENT

(TL:DS-69; 06-22-2000)

(**Prepare on Department or Post Letterhead Stationery**)

I hereby acknowledge personal receipt of the system password(s) and security standards associated with the user ID(s) listed below. I understand that:

(1) I am responsible for the protection of the password(s);

(2) I will comply with all applicable security standards; and

(3) I will not divulge my password(s).

I further understand that I should report to the Information Systems Security Officer (ISSO) any problem I may encounter in the use of the password(s) or when I have reason to believe that the private nature of my password(s) has (have) been compromised.

SYSTEM **USER ID**

____

____

____

____

____

User's Name (printed

name)______________________________Signature

__________________________ Date ___________ Position

____

Office/Post ______________________ Work Phone _________

System Manager (printed name) __________________________

Signature _______________________ Date _____________